Testimony

John "Neal" Latta

Assistant Administrator for Enrollment Services and Vetting Programs

Transportation Security Administration

U.S. Department of Homeland Security

FOR A HEARING ON

"Evaluating High-Risk Security Vulnerabilities At Our Nation's Ports"

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

May 10, 2023

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. Thank you for inviting me to testify on port security, specifically the Transportation Security Administration's (TSA) role in vetting maritime transportation workers for the Transportation Worker Identification Credential (TWIC) program. My testimony will highlight TSA's security responsibilities and achievements in the maritime environment and how TSA is working to enhance transportation security while bolstering customer service and supporting the flow of commerce.

TSA's Role in Securing the Maritime Environment

TSA is committed to securing the Maritime Transportation System (MTS), including waterways, ports, and land-side connections, against evolving and emerging risks, such as physical and cyber intrusions. TSA partners with public and private sector stakeholders, such as U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), port owners and operators, and national trade and labor associations, to secure the MTS from potential security threats.

TSA's Enrollment Services and Vetting Programs (ESVP) office administers TSA's enrollment, vetting, and credentialing programs, including the end-to-end program management and oversight of the technology, operations, and resources that support TSA's Security Threat Assessment (STA) programs. The TWIC program is an STA program designed to mitigate insider threats. These vetting programs are the foundation for identifying potential threats to U.S. critical infrastructure, and TSA prioritizes the vetting and adjudication of its worker populations to minimize impediments to the economy, industry, and the workforce. Specific to maritime security, TSA vets over 2.2 million maritime transportation workers, such as longshoremen, merchant mariners, truck drivers, engineers, and individuals in other occupations who require a TWIC STA for access to secure areas of port facilities and vessels.

TWIC Overview

The TWIC program is a fee-based Department of Homeland Security (DHS) security program mandated by the *Maritime Transportation Security Act of 2002* (MTSA), which mandates that individuals requiring unescorted access to MTSA-regulated facilities and vessels

must be issued a biometric transportation security card once the individual is determined not to pose a risk to transportation or national security. TWIC, jointly administered by TSA and USCG, is one of several layered security measures incorporated by federal, state, and local partners to prevent potential security breaches and incidents targeting U.S. critical and maritime infrastructure. Since the TWIC program was established in 2007, TSA has enrolled over seven million transportation workers.

TWIC and the Security Threat Assessment Process

TSA is responsible for enrolling and vetting applicants, adjudicating the STA, and issuing the biometric credential. The USCG administers the security program and TWIC access control standards for facility and vessel owners and operators to implement. Facility and vessel operators determine who is authorized to access secure areas of their MTSA-regulated facilities or vessels and verify that each individual holds a valid TWIC. Authorized access requires three functions to be performed: verification that an individual has undergone an STA, identity management, and establishment of the individual's business purpose.

TSA and its enrollment provider oversee more than 570 enrollment centers nationwide, including all 50 states, the District of Columbia, and U.S. territories. Following the collection of biometric (i.e., fingerprints and facial photograph) and biographic information, TSA creates a TWIC record in its case management system and performs the vetting of applicants for criminal history, intelligence/ties to terrorism, and lawful presence. Based on the vetting results, TSA adjudicates the case based on the interim and permanent disqualifying factors listed in TSA's regulations in 49 CFR Part 1572.

TSA's case management system adjudicates most TWIC applicants—approximately 60 percent of total enrollments—within 24 hours and an applicant receives their TWIC card via mail within seven to 10 business days. Approximately 40 percent of enrollments are considered complex cases due to a potentially disqualifying factor. Processing these cases may take TSA up to 30 to 60 days to make a determination. While most of these cases will ultimately result in the applicant receiving a TWIC, some applicants will be notified that they have been potentially disqualified. All TWIC applicants are afforded an opportunity to participate in the TSA redress process, which allows individuals to appeal TSA's initial decision or request a waiver.

TWIC Contributions to the Movement of Commerce

TSA mitigates security risks to maritime transportation by recurrently vetting TWIC holders to ensure individuals who pose a potential threat to transportation and national security cannot access secure areas. TSA continually strives to enhance its identity management and vetting capabilities. For example, in 2021, TSA began subscribing all new TWIC holders in Federal Bureau of Investigation Rap Back Services. This automation provides TSA with more accurate and real-time information on TWIC holder criminal activities after enrollment.

To facilitate the movement commerce, TSA has partnered with supply chain and maritime stakeholders to alleviate potential bottlenecks where TWIC or other TSA vetting programs could impede such movement. For example, in 2021, DHS and TSA contributed to the White House Supply Chain Disruptions Task Force and met with representatives at the Ports of Los Angeles and Long Beach, California, to discuss strategies to support essential workers accessing port terminals. TSA took immediate steps to address the needs of its maritime partners, including expanding enrollment center operations, expediting the vetting of mission-critical transportation workers, and reducing the time and burden associated with obtaining a TWIC.

Customer Experience

Customer service and engagement are critical success factors for TSA's STA programs. TSA recognizes transportation worker populations require efficient services from TSA to obtain and retain certifications, occupations, and professions. TSA is focused on enhancing the security value of its program while reducing the burden of obtaining a TWIC.

In 2009, TSA implemented TWIC One Visit which enables eligible workers to receive their TWIC card at a designated address instead of returning to an enrollment center for pick-up and activation. Today, 91 percent of total TWIC applicants receive their card via mail. In August 2022, TSA implemented a new online renewal capability for most TWIC applicants who maintain or previously maintained an active TWIC STA. Approximately 54 percent of active TWIC cardholders enroll for a new TWIC after their STA expires five years from the date of issuance. Of those workers renewing a TWIC, nearly 80 percent are using TSA's online renewal capability, thereby eliminating the cost and time burden associated with traveling to a physical

enrollment center. TWIC One Visit and online renewal grant maritime workers their TWICs faster, allowing them to fulfill their roles in transportation security more expediently.

In addition, due to the reduced costs associated with the online transaction, TWIC applicants now pay a reduced fee when renewing their credentials online: $117.25, compared to the in-person fee of $125.25. Since TSA issued the first TWIC in October 2007, TSA has not increased the enrollment fee for TWIC applicants.

Conclusion

TSA continues to work to improve and enhance maritime security through its TWIC program. Chairman Gimenez, Ranking Member Thanedar, and members of the Subcommittee, thank you for the opportunity to appear before you today. I look forward to your questions.

Testimony

Eric Goldstein
Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Evaluating High-Risk Security Vulnerabilities At Our Nation's Ports"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

May 10, 2023

Chairman Giménez, Ranking Member Thanedar, and members of the Subcommittee: Thank you for the invitation to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA). CISA leads the national effort to understand, manage, and reduce risk to our critical infrastructure. This mission is grounded in partnership with each Sector Risk Management Agency and critical infrastructure operators in each sector. While each sector is uniquely critical, the Maritime Transportation Sub-Sector, and the nation's ports represented therein, serves as a linchpin of our nation's prosperity and security. For this reason, our work with the U.S. Coast Guard and the maritime community is uniquely essential. I appreciate this opportunity to discuss the cybersecurity elements of CISA's work on port security.

From Miami to Detroit, and from the Gulf Coast to the Pacific, America's ports drive our economic and national security. Maritime transportation accounts for the single largest share of U.S. trade, both supplying our households and businesses with necessities and facilitating trade that supports American jobs. We have seen in the past few years how disruptions to maritime commerce, regardless of cause, can produce significant impacts for businesses and consumers, and we recognize that America's ports are equally critical in enabling our armed forces to effectively deploy and supply.

At CISA, we share the Subcommittee's concern regarding threats to ports posed by the government of the People's Republic of China (PRC), which could manifest in multiple forms. We continue to work urgently with the Coast Guard and the port community to understand and mitigate these threats, whether from critical equipment manufactured by Chinese state-owned enterprises or the prospect of damaging cyber intrusions targeting port infrastructure. These threats catalyze our focus, clarify our intent, and underpin our shared investment.

Partnership with the United States Coast Guard and the Transportation Security Administration

Our nation's maritime system is highly complex, and no one organization maintains the authorities, resources, or capability to bear the burden of securing these systems alone. Our partnership with both the Coast Guard and the Transportation Security Administration (TSA) are foundational in achieving our shared mission. The Coast Guard and TSA play leading roles in operationalizing the Department of Homeland Security's responsibilities as a co-Sector Risk Management Agency for the Transportation Systems Sector. CISA coordinates with the Coast Guard and TSA to advance this work in several ways.

First, we must provide members of the maritime community, including port operators, with actionable information to protect their systems. For this reason, CISA and the Coast Guard frequently engage in joint amplification or development of combined products for this community, with recent examples including CISA's amplification of a Coast Guard Safety Alert

with recommended cybersecurity best practices for commercial vessels and a joint advisory regarding malware exploiting the Log4Shell vulnerability. In addition, the Coast Guard was a key partner in our development of the Cross-Sector Cybersecurity Performance Goals (CPGs), which provide a straightforward and actionable set of cybersecurity actions prioritized by cost, impact, and complexity and organized around the National Institute of Standards and Technology Cybersecurity Framework. The CPGs are a foundational tool to help any organization align limited cybersecurity resources toward the most impactful investments. We look forward to partnering closely with the Coast Guard to develop sector-specific goals for maritime stakeholders that reflect the unique technology and risk considerations of the sub-sector.

Second, the Coast Guard and TSA are key participants in Cyber Storm, CISA's annual national capstone cyber exercise that brings together the public and private sectors in a simulated response to a cyber crisis impacting the nation's critical infrastructure. During the current Cyber Storm exercise series, the Coast Guard and TSA are participating within working groups of federal entities to respond to a simulated cyber threat. These exercises foster collaboration and communication across agencies to ensure that federal and non-federal entities are ready to collectively respond to major cyber incidents.

Finally, CISA, the Coast Guard, and TSA coordinate through formal mechanisms to promote critical infrastructure security. All three agencies are members of the Maritime Modal Subsector Government Coordinating Council (GCC) under the Critical Infrastructure Partnership Advisory Council framework, which provides a forum for federal agencies to collaborate with one another and to seek private sector input. Specifically, the Maritime Modal Subsector GCC allows federal agencies to collaborate on strategies for mitigating risk to ports and other elements of the maritime transportation sub-sector. Through this coordinating council and other channels, CISA, the Coast Guard, and TSA stay connected with one another and with non-federal entities to support collective efforts to mitigate cybersecurity and other risks to ports.

Supporting Our Partners to Actively Reduce Risk

CISA also works directly with ports and other critical infrastructure entities to support their cybersecurity efforts. By leveraging our expertise, our ability to generate efficiencies of scale, and our ability to cross-reference information from multiple sources to gain broad visibility into the cyber threat environment, CISA is uniquely positioned to assist critical infrastructure operators with mitigating cybersecurity risk.

As a key part of this effort, we enable network owners and operators to harden their networks against known and potential tactics, techniques, and procedures used by PRC cyber actors. For example, we published in late 2022 a joint advisory with the National Security Agency and the Federal Bureau of Investigation outlining the vulnerabilities most frequently used by PRC actors, enabling organizations around the country to close down intrusion paths commonly used by the

PRC to achieve their strategic goals. We regularly scan over 5,000 federal, critical infrastructure, and state, local, tribal, and territorial (SLTT) partners' networks upon their request to identify the presence of these vulnerabilities and notify identified entities to prioritize urgent mitigation. More recently, we have undertaken an effort intended to make network owners and operators aware of the prevalence of devices produced by PRC-based vendors that are listed on the Federal Communications Commission's "Covered List," which, under the Secure and Trusted Communications Networks Act of 2021, pose an "unacceptable risk to the national security of the United States or the security and safety of United States persons." Using commercial tools, we have identified such products used on critical infrastructure networks across the country and have already notified 88 critical infrastructure organizations using such products about the potential associated risks. In nearly all cases, the notified entities have chosen to take urgent steps to replace these products from their networks and reduce the likelihood of unauthorized access by PRC actors.

We are particularly focused on proactive efforts to reduce the likelihood that our partner entities will experience serious cybersecurity incidents. We have enrolled a select group of our nation's most critical infrastructure entities in the CyberSentry program, a voluntary effort that uses commercial off-the-shelf tools and equipment to identify and detect malicious activity targeting critical infrastructure corporate and industrial control systems networks. This program has yielded significant operational benefits among participating entities, and we look forward to expanding into the maritime sub-sector in the next year. Further, our Vulnerability Scanning service helps organizations identify and address vulnerabilities, particularly those that are known to be exploited by adversaries. In addition, we have over 100 cybersecurity personnel across the country to provide guidance, assistance, and a front door to CISA's broader portfolio of risk reduction services. These regional personnel are working every day to build relationships with the maritime community to understand what these stakeholders need and ensure that CISA provides every possible resource to support their cybersecurity efforts.

CISA also has an important role in helping critical infrastructure entities prevent the worst outcomes after a cyber intrusion has occurred. We leverage information from partners and security researchers to notify victims so that they can take action to contain and eradicate the threat. Our new Pre-Ransomware Notification Initiative identifies organizations that ransomware actors have compromised and aims to notify them before their data is encrypted or stolen, with over 160 having been notified so far. Once we receive information about a compromised organization, our field personnel take urgent action to notify the victim organization and provide specific mitigation guidance. CISA also provides direct support to victims of cyber incidents through incident response services.

Looking to the future, CISA is continuously developing new capabilities to help our stakeholders drive down cyber risk based upon their feedback and needs. We are looking forward to several

impactful new efforts in the coming months, including an effort that will expand one of our cybersecurity shared service offerings beyond the federal sphere to certain critical infrastructure entities, a new attack surface management service, and a modernized cyber threat intelligence service. Through each of these efforts, we will work closely with the maritime community to understand their needs and maximize our ability to deliver services, information, and guidance that helps our partners detect, prevent, and effectively respond to cyber risks.

Getting Ahead of the Threat

Another pillar of CISA's cybersecurity work is our cybersecurity defense planning. This aligns with Congress's statutory direction for CISA to engage in joint planning with a range of critical infrastructure partners to create common, shoulder-to-shoulder approaches to confront malicious actors and significant cyber risks. To date, CISA's planning efforts have addressed topics including the cybersecurity implications of the Russian invasion of Ukraine and the creation of a framework for public-private crisis action planning. During 2023, CISA's planning agenda includes systemic risks posed by cyber intrusions against software and infrastructure that underlie multiple national critical functions, as well as updating the National Cyber Incident Response Plan. CISA will continue to engage transportation and maritime stakeholders in this work to ensure that it provides value for these key facets of our national infrastructure.

We take a strategic approach to reduce the likelihood of damaging intrusions, particularly those perpetrated by PRC actors. In so doing, we recognize a hard truth: most technology products used across American networks are neither secure by design nor by default, which makes it far too easy for malicious actors to find vulnerabilities and makes it far too hard for organizations to deploy necessary security measures. Recently we published a set of principles with six international partners that intends to catalyze progress toward further investments and cultural shifts necessary to achieve a safe and secure future. These principles aim for technology providers to take ownership of the security outcomes of their technology products, shifting the burden of security from the customers and ensuring executive level commitment for software manufacturers to prioritize security as a critical element of product development. This will be a long-term journey but a necessary one that will require all elements of society, from enterprises to technology providers to Congress, to join together in driving change.

Conclusion

Thank you again for this opportunity for CISA to testify on this important topic. I look forward to further discussion of how our Coast Guard and TSA partnership, our rapidly maturing capabilities, and our planning efforts advance the national imperative to secure our ports. I welcome any questions you may have.

U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL WAYNE R. ARGUIN
ASSISTANT COMMANDANT FOR PREVENTION POLICY

ON
EVALUATING HIGH-RISK SECURITY VULNERABILITIES
AT OUR NATION'S PORTS

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
TRANSPORTATION & MARITIME SECURITY SUBCOMMITTEE

10 MAY 2023

Introduction

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. I am honored to be here today to discuss a top priority for the U.S. Coast Guard: protecting the marine transportation system (MTS). At all times, the Coast Guard is a military service and branch of the U.S. Armed Forces, a federal law enforcement agency, a regulatory body, a co-Sector Risk Management Agency, a first responder, and a member of the U.S. Intelligence Community. We are uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

Since the early days of the Revenue Cutter Service, we have protected our Nation's waters, harbors, and ports. While much has changed over the centuries—with our missions expanding from sea, air, and land into cyberspace—our ethos and operational doctrine remain steadfast. We employ a risk-based approach to protect the Nation from threats in the maritime environment. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our workforce; and the breadth of our military, law enforcement, and civil partnerships to protect the Nation, its waterways, and all who operate on them.

The Criticality of the Marine Transportation System

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. The MTS' complexity and consequence to the Nation cannot be overstated. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. It is more than ports and waterways. It is cargo and cruise ships, passenger ferries, waterfront terminals, offshore facilities, buoys and beacons, bridges, and more. The MTS supports $5.4 trillion of economic activity each year and accounts for the employment of more than 30 million Americans. It protects critical national security sealift capabilities, enabling U.S. Armed Forces to project and maintain power around the globe. We remain laser-focused on the safety and security of the MTS as an economic engine and strategic imperative, and we continue to serve as the Sentinels envisioned at our founding.

Evaluating Vulnerabilities – A Shared Responsibility

Safeguarding the MTS requires diligent assessment and remediation of vulnerabilities. The Coast Guard works across multiple levels of industry and government to assess security vulnerabilities, determine risk, and develop mitigation strategies. This layered approach—from the local to the international level—is critical due to the size, diversity, and interconnectedness of the MTS.

Locally: Vessel and Facility Security Assessments

Security assessments in U.S. ports and waterways start with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) regulations in 33 CFR 104, 105, and 106 place specific requirements on regulated entities to conduct personalized security assessments, analyze the results, and prepare a security assessment report that is included in their security plans.

A completed security assessment report must be submitted to the Coast Guard as part of the plan approval process and include a description of how the on-scene survey was conducted, key facility operations to protect, each vulnerability found, security measures to address each vulnerability, and potential gaps in security policies and procedures.

In February 2020, the Coast Guard provided further guidance to the regulated industry on incorporating computer systems and networks into their required assessments and plans. During inspections to verify compliance, the industry sought more specific guidance on ways to integrate cyber into their existing security regime. The Coast Guard partnered with the Homeland Security Systems Engineering and Development Institute, a federally funded research and development center operated by the MITRE Corporation, and the National Maritime Security Advisory Committee (a Federal Advisory Committee) to develop the Maritime Cybersecurity Assessment and Annex Guide. This guide was released in January 2023 and provides a clear process for identifying and describing cybersecurity vulnerabilities, then addressing those vulnerabilities in mandated security plans.

For foreign ships operating in U.S. waters, the process is very similar to MTSA-regulated vessels and facilities. Per the International Ship and Port Facility Security Code (ISPS Code), each ship must conduct a Ship Security Assessment that identifies key shipboard operations to protect; threats to key shipboard operations; existing security measures and procedures; and potential weaknesses, including human factors, in security policies and procedures. This assessment then leads to the development of a Ship Security Plan, which must be approved by the ship's Flag Administration, and is verified by the Coast Guard during regular compliance examinations in U.S. ports.

Regionally: Area Maritime Security Assessments and Plans

At the regional level, Area Maritime Security Committees (AMSC) are required by federal regulations and serve an essential coordinating function during normal operations and emergency response. They are comprised of government agency and maritime industry leaders and serve as the primary regional body to jointly share threat information, evaluate risks, and coordinate risk mitigation activities. As the Federal Maritime Security Coordinator (FMSC), Coast Guard Captains of the Port (COTP) around the country direct their regional AMSC's activities.

The AMSC's input is vital to the development and continuous review of the Area Maritime Security (AMS) Assessment and Area Maritime Security Plan (AMSP). The AMS Assessment must include the critical MTS infrastructure and operations in the port; a threat assessment that identifies and evaluates each potential threat; consequence and vulnerability assessments; and a determination of the required security measures for the three Maritime Security levels.

These AMS assessments then lead to the collaborative development of AMSPs to ensure government and industry security measures are coordinated to deter, detect, disrupt, respond to, and recover from a threatened or actual Transportation Security Incident (TSI).

The COTP/FMSC and the AMSC ensure that a formal AMS Assessment for their entire Area of Responsibility (AOR) is conducted at least every five years. The AMS Assessment must also be evaluated at least annually to ensure its adequacy, accuracy, and consistency.

Nationally: Interagency Coordination and Assessment

As outlined in Presidential Policy Directive 21, along with the Department of Transportation, the Coast Guard is the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector. As a SRMA, the Coast Guard is responsible for coordinating risk management efforts with the Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner in all our risk management activities. CISA's technical expertise directly supports the Coast Guard's ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA integrates a whole-of-government response, analyzes broader immediate and long-term impacts, and facilitates information sharing across transportation sectors. The relationship with CISA is strong and will continue to mature.

As a member of the U.S. Intelligence Community, the Coast Guard provides unique authorities, opportunities, and capabilities to collect, fuse, analyze, and share information and intelligence across domestic and international government and non-government stakeholders throughout the MTS. The Coast Guard's intelligence authorities allow for a collective understanding of factors and entities affecting the maritime domain, including physical security and cybersecurity. Threats, such as ransomware attacks, continue to mature in effectiveness and prevalence, requiring the Intelligence Community to align resources and integrate efforts that protect the safety and security of the MTS.

The enduring relationship with the Department of Defense (DoD) is also crucial to safeguarding the MTS. In many cases, DoD's ability to surge forces from domestic to allied seaports depends on the same commercial maritime infrastructure as the MTS. The relationship between the Coast Guard and DoD ensures the Nation's surge capability and sea lines of communication will be secure and available during times of crisis. By sharing threat intelligence, developing interoperable capabilities, and using DoD's expertise, the Coast Guard enables national security sealift capabilities and jointly supports our Nation's ability to project power around the globe.

The Coast Guard serves as a partner to the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject matter expertise in maritime security. FEMA is responsible for the administration and management of the program, which includes designing and operating the administrative mechanisms and managing the distribution

and tracking of funds. The PSGP is designed to support AMSPs and facility security plans (FSPs) to protect critical port infrastructure from terrorism. All U.S. ports are eligible for PSGP funding. PSGP funds are intended to offset the costs for maritime security risk mitigation projects borne by maritime partners. To date (FY 2002 – FY 2022), the PSGP distributed over $3.73 billion to port stakeholders to make security improvements, including assisting facilities with capital investments for MTSA compliance.

Internationally: International Port Security Program

Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, and through the Coast Guard International Port Security (IPS) program, the Coast Guard conducts in-country foreign port assessments and applies the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to assess the effectiveness of security and anti-terrorism measures in foreign ports.

If the Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, we may impose Conditions of Entry (COE) that define additional security measures that vessels arriving to the United States from those ports must implement. COE may result in security verifications of vessels before they enter U.S. ports to verify that additional security measures were taken in foreign ports. The IPS program also conducts capacity building engagements to assist countries in implementing effective anti-terrorism measures.

The U.S. Coast Guard's Approach

To support the whole-of-government effort, the Coast Guard applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. Coast Guard authorities and capabilities cut across threat vectors, allowing operational commanders at the port level to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions. It begins with establishing expectations in the MTS. Regulations and standards provide a set of baseline requirements and are critical to establishing effective and consistent governance regimes. With effective standards in place, compliance activities systematically verify that the governance regime is working. This part of the system is vital in identifying and correcting potential risks before they advance further and negatively impact the MTS. Effective assessment is paramount to continuous improvement. It provides process feedback and facilitates the identification of system failures so that corrective actions can be taken to improve standards and compliance activities.

Importantly, the Coast Guard operationalizes this framework at the port level. Coast Guard COTPs oversee MTSA-regulated vessels and facilities through their mandated Vessel or Facility Security Assessments and Plans. These plans set baseline activities to protect the MTS through personnel training, drills and exercises, communication, vessel interfaces, security systems, access control, cargo handling, delivery of stores, and restricted area monitoring.

The Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These new positions create a dedicated staff to build and maintain port level security-related relationships, facilitate information sharing across industry and government, advise Coast Guard and Unified Command decision-makers, and plan security exercises.

Response

Similar to the Prevention Concept of Operations, the Coast Guard has a proven, scalable response framework that can be tailored for all hazards. This is especially important as cyber incidents can quickly transition to producing physical impact, requiring operational commanders to immediately deploy assets to mitigate risks. Depending on the incident's size and severity, commanders will set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response. The Service is not approaching this alone.

By regulation, MTSA-regulated vessels and facilities are required to report TSIs, breaches of security, and suspicious activity without delay. These reports enable operational commanders to rapidly notify other government agencies, evaluate associated risks, deploy resources, and unify the response.

For complex responses, the Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of prevention and response needs. These teams include specially trained law enforcement teams that can bolster physical security, pollution response teams for significant oil spills or hazardous material releases, and Cyber Protection Teams that can help local responders navigate the highly technical aspects of cyber incident assessment and response.

Through both prevention and response activities in the field, and engagements with industry, the Coast Guard captures lessons learned, recommendations, and best practices that strengthen the maritime industry's security posture and inform future policy, law, and regulations.

Future Focus

Working in close collaboration with CISA and other government partners, foreign allies, and industry, the Coast Guard will continue to leverage strong and established relationships across the maritime industry – at all levels – to assess and address security vulnerabilities.

The Coast Guard has secured and safeguarded the maritime environment for over 230 years and, during that time, has faced many complex challenges. We have honed our operating concepts, bolstered our capabilities, and strengthened our resolve. These same concepts and capabilities will secure and protect the Nation and maritime critical infrastructure from malicious activity in all domains. In addressing risks to ports and other components of the MTS, the Coast Guard's commitment is to address those risks with the same level of professionalism, efficiency, and effectiveness that the public has come to expect.

Thank you for the opportunity to testify today and thank you for your continued support of the United States Coast Guard. I am pleased to answer your questions.